IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Elijahu Shapira

Serial No.:   09/934,994

Filed: August 21, 2001

For: DATA TRACKING USING IP ADDRESS FILTERING
OVER A WIDE AREA NETWORK

Date: April 28, 2006

Confirmation No. 9111

Examiner: Lashonda T. Jacobs

Group Art Unit: 2157

MAIL STOP Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**APPELLANT'S BRIEF
UNDER 37 C.F.R. § 41.37**

Appeal is taken from the Examiner's Office Action mailed November 30, 2005, finally rejecting claims 1-13 in the instant application.

This Appeal Brief is in furtherance of the Notice of Appeal mailed in this case on February 28, 2006.

The fees required under §41.37(a)(2) and any required petition for extension of time for filing this Brief and fees therefor are dealt with through the payment section of the electronic filing system.

This Brief contains these items under the following headings, and in the order set forth below.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST
37 CFR § 41.37(c)(1)(i)

The real party in interest in this appeal is WebTrends Inc., the assignee of the above-referenced patent application.

II. RELATED APPEALS AND INTERFERENCES
37 CFR § 41.37(c)(1)(ii)

There are no other appeals or interferences known to Appellant, the Appellant's representative, or assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS
37 CFR § 41.37(c)(1)(iii)

1.   Claims presented: 1-13

2.   Claims rejected: 1-13

3.   Claims allowed or confirmed: NONE

4.   Claims withdrawn: NONE

5.   Claims objected to: NONE

6.   Claims cancelled: NONE

All the rejected claims, Claims 1-13, are being appealed. The appealed claims are eligible for appeal, having been finally rejected.

IV. STATUS OF AMENDMENTS
37 CFR § 41.37(c)(1)(iv)

Subsequent to the last Office Action mailed on November 30, 2005, which contained a Final Rejection of the appealed claims, no further amendments have been filed.

V. SUMMARY OF CLAIMED SUBJECT MATTER
37 CFR § 41.37(c)(1)(v)

There are two independent claims 1 and 7 involved in this appeal.

The claims in the instant application are directed to the application of preset IP filters in the compilation and reporting of data associated with traffic activity to web pages.

The independent claims are of various scope and claim overlapping features.

Claim 1, for instance, is a method for generating web traffic reports and includes presetting IP filters and storing a web page on a first server coupled to a wide area network, whereby the web page including data mining code. The web page would then be uploaded to a visitor computer responsive to a request over the wide area network from the visitor computer, whereby the visitor computer would have a designated IP address. The data mining code would then be operated on the visitor computer to obtain technical data. A subsequent step would be receiving at a second server the technical data and the IP address of the visitor computer and generating a log file incorporating the technical data and IP address. The IP filters would be applied to the IP address stored in the log file and a database file would then be generated from the log file responsive to the IP filters.

Claim 7 is a network which includes a visitor node having a browser program coupled to the network, whereby the visitor node provides requests for information on the network. The network further includes a web site node having a respective web site responsive to requests for information from the visitor node to provide media content and data mining code to the visitor node. The apparatus also includes a tracking node including a log file and a database. The tracking node is responsive to a communication from the visitor node based upon the data mining code to store visitor data obtained from the visitor node into the log file. Finally, the apparatus network includes a filter node responsive to the visitor data based on a filter to select the visitor data for storage in a data base, whereby said data base is accessible by an owner of the web site node to view relevant traffic data to the web site node.

The stated purpose of such a system and method is to provide web site traffic analysis reports that ignore visits from disfavored visitors. For instance, if a company is interested in knowing the extent of meaningful commercial traffic to the company's web site, then IP filters can be set that allow the company to ignore visits from the company's own employees.

The filters can be set in advance (*e.g.* "preset filters") so that filtering happens automatically prior to report generation, thus saving having a new report run at the time of request.

Each independent claim is directed to different aspects of the invention and each stand and fall, independently, with their associated dependent claims.

A. Independent Claim 1

Claim Language	Support in Specification/Figures
A method for generating web traffic reports comprising the steps of:	FIG. 4 flow chart.
presetting IP filters;	FIG. 3B IP addresses typed into data field for "exclude" variant. FIG. 4, block 30.
storing a web page on a first server coupled to a wide area network, said web page including data mining code;	- web page (FIG. 2) - first server (FIG. 1, element 12) - wide area network (FIG. 1, element 10) - example data mining code listed in Appendix I and II in specification; also p. 9, lines 4-22 of specification.
uploading the web page to a visitor computer responsive to a request over the wide area network from the visitor computer, said visitor computer having a designated IP address;	- uploading to visitor computer in FIG. 4, block 32. - visitor computer (FIG. 1, element 14) - IP addresses discussed in application, page 6, line 17 to page 8, line 31.
operating the data mining code on the visitor computer to obtain technical data;	Operating code to obtain technical data on p. 9, lines 4-22. Also, FIG. 4, block 34.
receiving at a second server the technical data and the IP address of the visitor computer and generating a log file incorporating the technical data and IP address;	FIG. 4, block 36. - Second server (FIG. 1, element 20) - Log file (example shown in page 9, lines 10-12). Also FIG. 4, block 40.
applying the IP filters to the IP address stored in the log file; and	Filters set in FIG. 3B applied to log files on analysis server 22 (application, page 9, lines 33 to page 10, line 13). Sample code shown in Appendix IV.
generating a database file from the log file responsive to the IP filters.	Generating files in FIG. 4, block 48. Database files results in reports FIGs. 5A, and 5B. See also page 10, lines 7-13.

B. Independent Claim 7

Claim Language	Support in Specification/Figures
A network comprising:	FIG. 1.
a visitor node having a browser program coupled to said network, said visitor node providing requests for information on said network;	- visitor node (FIG. 1, element 14) - application page 3, lines 28-30.
a web site node having a respective web site responsive to requests for information from said visitor node to provide media content and data mining code to said visitor node;	- web site node (FIG. 12, element 12) - web site (FIG. 2) - data mining code (Appendix I and II)
a tracking node including a log file and a database, said tracking node responsive to a communication from said visitor node based upon said data mining code to store visitor data obtained from said visitor node into said log file; and	- tracking node (FIG. 1, elements 20, 22, 24) - FIG. 4, block 36. - Second server (FIG. 1, element 20) - Log file (example shown in page 9, lines 10-12). Also FIG. 4, block 40.
a filter node responsive to said visitor data based on a filter to select said visitor data for storage in a database,	Filters set in FIG. 3B applied to log files on analysis server 22 (application, page 9, lines 33 to page 10, line 13). Sample code shown in Appendix IV.
whereby said database is accessible by an owner of said web site node to view relevant traffic data to the web site node.	Generating files in FIG. 4, block 48. Database files results in reports FIGs. 5A, and 5B. See also page 10, lines 7-21.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
37 CFR § 41.37(c)(1)(vi)

A. Claims 1-13 stand rejected under 35 U.S.C. §102(e) as being anticipated by Muret, et al. (U.S. Patent No. 6,804,701).

VII. ARGUMENT
37 CFR § 41.37(c)(1)(vii)

The general issue is whether claims 1-13 are unpatentable under 35 U.S.C. § 102(e) in view of a single prior art reference: U.S. Patent No. 6,804,701 (Muret). Briefly, the specific issues can be stated as follows:

    A. Muret fails to disclose, *inter alia*, the following elements of the independent claims including:

        a. A step of "presetting IP filters" [Claim 1]

        b. A step of "storing web pages . . . including data mining code" [Claim 1]

c. A "filter node responsive to said visitor data based on a filter to select said visitor data for storage in a database" [Claim 7]; and

d. A web site including "data mining code" [Claim 7]

e. A "tracking node responsive to communication from a visitor node." [Claim 7]

These issues will be divided into respective subsections and will address each of the grounds for rejection separately.

Claims 1-13 are pending in the application as originally filed. A first Office Action issued with all claims rejected under 35 USC §103(a) as being unpatentable over various combinations of prior art references including McCreery et al. (U.S. Patent No. 5,787,253), Henrick et al. (U.S. Patent No. 6,055,510), Reilly et al. (U.S. Patent No. 5,740,549), and Dobbins et al. (U.S. Patent No. 6,249,820). Applicants arguments resulted in the rejections being withdrawn and new grounds for rejection imposed in view of new art not previously cited by the Examiner.

Claims 1-13 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,804,701 (Muret, et al.).

Because of clear differences between the Muret reference and the claimed elements of the current invention, no amendments are considered necessary for allowance over the prior art at issue and, consequently, no changes have been made to the claims. Accordingly, reconsideration and allowance of all claims is respectfully requested in view of the following remarks.

Two independent claims (1 and 7) are pending in the current application. The following remarks address the absence of certain features of these claims in the Muret patent. In particular:

A. *Muret Fails to Teach the Step in Claim 1 of "Presetting IP Filters" or the "filter node" claimed in Claim 7*

In addressing the claim 1 limitation calling for the step of "presetting IP filters," the Examiner refers to the following portions of Muret:

I. Log Parser Module (210)

> FIG. 4 is a flowchart and schematic diagram illustrating a preferred control routine for the log parser module 210 of FIG. 3, configured to process static log files 510. One of the most time consuming operations is reading and processing the raw log files 510. With individual log files 510 containing potentially over a gigabyte of data, getting the raw data into the system 100 is an important step.

> The purpose of the log parser module 210 is to efficiently read each log line 512 and separate it into its individual fields. The fields can include the IP address, timestamp, bytes sent, status code, referral, etc. As discussed above, each log line 512 in the log file 510 represents a hit or transaction from one of the web servers 500.
> (Muret, Col. 7, lines 58 through Col. 8, line 3)

II. The user interface 4000 preferably includes a navigation area 4040 that contains a collection of menus that group the available reports into different categories, preferably seven main categories, each with an associated link 4050: Traffic; Pages; Referrals; Domains; Browsers; Tracking; and E-Commerce. A collection of links to specific reports 4060 related to a chosen category link 4050 is preferably displayed under a chosen category link 4050. The currently chosen report link 4070 is preferably indicated by a change in color Or shading. In the example shown in FIG. 28, the currently chosen report link 4070 corresponds to the "Snapshot" report.

> The user interface 4000 preferably includes a "date range" functions area 4080. Depending on the report chosen, this date range functions area 4080 allows the user to select the date range of the report being shown. The user interface also preferably includes a controls area 4090 that preferably includes preferences and report exporting features. The preferences function of the controls area 4090 allows the user to change report settings, such as the language that is used for display. The exporting function of the controls area 4090 allows the user to export the currently viewed data for use in other applications, such as Microsoft Excel™.
> (Muret, Col. 26, line 54 through Col. 27, line 9)

The above text (I) only states that the IP address of the visitor computer can be a field in the log file stored at the web server. The above text (II) states only that reports may be grouped into different categories, but that such reports are _static_ rather than real time as is possible under the current invention. (see, _e.g._, Muret, Col. 26, lines 42-45). Dynamic, real-time reports are available under Muret, but only under the scheme noted in FIGS. 22-25. Muret, Col. 25, lines 25-38 note the use of IP numbers in processing log files, but it is clear that records using all such log files are used. IP _filters_ are not mentioned in Muret. In fact, the word "filter" occurs only once in Muret [Col. 6, line 67] and only then refers to website identification by use of regular expression filters. The remainder of the Muret application references three methods for obtaining the visitor IP address, including (1) a web server logging the IP address of the visitor, (2) using DNS to resolve the host and domain information, or (3) using a DNS Resolver Module (260) operable on the Muret web traffic analyzer 100. [see, _e.g._, Col. 13, lines 19-57] None of the methods for resolving the IP address involve setting filters.

Even more importantly, there is no reference or suggestion within Muret that IP filters should be preset. In the present application, the invention addresses the problem of discounting irrelevant visitors to a particular web site (_e.g._, from the company's own computers) when establishing pertinent traffic data. This problem is stated in the specification of the present application at page 2, lines 4-10.

A clear difference in Muret is apparent by comparing the explicit language within Muret with the teachings of the present invention:

Muret	Present Invention
"The record is updated with the information from the log line." (Muret, Col. 25, lines 38-39)	"If the IP address is either not on the INCLUDE list or is on the EXCLUDE, then the log file is ignored and the database is not updated." (Application, page 10, lines 10-11)

Muret does not address the problem with IP filtering, does not present a solution for web filtering, and in fact does not appear to even allow a preset filter to be incorporated within the data analyzing tool used to parse the data and provide a web traffic report. Any parse function that could be applied to the web log data to display IP addresses of visitors to specific web sites under Muret would have to be enacted after the data is collected. There is no function recited within Muret that would allow a filter on the IP data to be implemented prior to collection of the data (*e.g.*, "presetting...").

Whereas Muret does not filter by IP address, the present invention as claimed does. The advantage of performing the filter on the log file as in the present invention is that undesired data is not included within the report/database in the first instance, thus saving computational resources. In other words, log files associated with undesired IP addresses are ignored and the database is not updated. Even if post-processing on the Muret-obtained data records were to filter by IP addresses, such post-processing would not result in the present invention's advantage of conserving resources. Furthermore, real-time data would not be available as there would always be a lag between when the report is requested and when compiled under Muret since a post-processing filter would be required.

The filter node element in claim 7 acts responsive to the visitor data (*e.g.*, IP address) to "select said data for storage in a database." As Muret does not include such filters, but rather stores ass such log files in records (see, *e.g.*, Muret Col. 25, lines 25-38), no such feature is taught by the Muret reference.

As there are missing elements from the prior art of record, rejection of pending claims under 35 USC §102(e) would therefore be inappropriate in this case and reversal of the rejection is required.

B. *Muret Fails to Operate With a Web Page That Includes "Data Mining Code"*

In addressing the claim 1 limitation calling for the step of storing a web page on a first server where the web page includes "data mining code," the Examiner refers to the following portion of Muret:

> Extremely busy websites will often use an array of servers to handle the extreme load of traffic. Other websites may have a secure server area that resides on a special machine.
>
> Whether for robustness or functionality, multiple server architecture is a common practice and appears to create a unique problem for internet traffic analysis and reporting. Each web server 500 will create its own log file 510, recording entries from visitors as they travel through the website. Often, a single visitor will create log entries in the log file 510 for each web server 500, especially if the web servers 500 perform different functions of the website.
> (Muret, Col. 10, lines 58-67)

Muret operates by querying the web servers for log file data rather than receiving data directly from the visitor computers themselves via data mining code embedded within the web pages sent from the web servers. It is clear from the citation in Muret above that the web servers themselves create the log files from web page visits. There is no mention in Muret that the web pages themselves served to the visitors would include data mining code that obtains this information. A more appropriate description of Muret is that the web <u>server</u> has stored thereon some sort of data mining code, but that the web <u>pages</u> it serves do not include such code.

Furthermore, as no data mining code is transferred with the Muret web page, the "operating the data mining code on the visitor computer" step cannot be performed. Since the Muret web pages do not include data mining code, these claim 1 limitations are not found in Muret and rejection under §102(e) would be inappropriate.

Claim 7 additionally includes a web site node operable to provide media content and data mining code to the visitor node. As data mining code is not provided to the visitor under the web server data record keeping of the Muret system, claim 7 would not be anticipated by Muret.

The Examiner's statement in the Final Office Action sheds no light on where in Muret it is taught that a web page has data mining code embedded within it. The Examiner simply states that, "it is obvious that data mining code is being used in Muret because the system is monitoring, tracking, and collecting raw data in order to generate reports." Again, Appellant is not stating that Muret does not infer some sort of data mining operation, as such obviously takes place on the Muret servers. Instead, Appellants state simply that Muret does not teach the explicit language in the claims: that the web page include data mining code [claim 1] and that a web site is adapted to provide data mining code to the visitor node [claim 7].

C. Muret Is Incapable of Enabling a Tracking Node as Claimed in Claim 7

Finally, claim 7 further requires a tracking node responsive to communication from a visitor node. The topography of the Muret system does not allow direct communication between the web site visitor and the data tracking system (100) as shown in Muret FIGs. 1 and 2. Accordingly, such an element is not shown in Muret and claim 7 should be allowable over the prior art of record.

VIII. CLAIMS APPENDIX
37 CFR § 41.37(c)(1)(viii)

A copy of the claims involved in the appeal, Claims 1-13, are attached hereto as an appendix, entitled Claims Appendix.

IX. EVIDENCE APPENDIX
37 CFR § 41.37(c)(1)(ix)

No evidence was submitted pursuant to 37 CFR §§ 1.130, 1.131 or 1.132 of this title, nor was any other evidence entered by the Examiner and relied upon by the Appellant in the appeal.

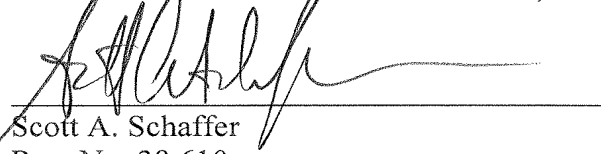## X. RELATED PROCEEDINGS APPENDIX
37 CFR § 41.37(c)(1)(x)

No related proceeding was identified pursuant to 37 CFR § 41.37(c)(1)(ii) of this section.

CONCLUSION

For the foregoing reasons, Appellant requests that the Board reverse the Examiner's rejections to Appellant's claims.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Scott A. Schaffer
Reg. No. 38,610

MARGER JOHNSON & McCOLLOM, P.C.
210 SW Morrison Street, Suite 400
Portland, Oregon 97204
(503) 222-3613

The text of the claims on appeal, 1-13, are as follows:

1.   A method for generating web traffic reports comprising the steps of:

presetting IP filters;

storing a web page on a first server coupled to a wide area network, said web page including data mining code;

uploading the web page to a visitor computer responsive to a request over the wide area network from the visitor computer, said visitor computer having a designated IP address;

operating the data mining code on the visitor computer to obtain technical data;

receiving at a second server the technical data and the IP address of the visitor computer and generating a log file incorporating the technical data and IP address;

applying the IP filters to the IP address stored in the log file; and

generating a database file from the log file responsive to the IP filters.

2.   The method of claim 1, wherein the step of presetting IP filters includes setting an INCLUDE IP filter.

3.   The method of claim 1, wherein the step of presetting IP filters includes setting an EXCLUDE filter.

4.   The method of claim 1, wherein the step of applying the IP filters to the IP addresses includes the step of using classless inter-domain routing.

5.   The method of claim 1, wherein the step of applying the IP filters to the IP addresses includes the step of using standard pattern matching specifications like Regular Expressions.

6.   The method of claim 1 further including the steps of:

defining a subnet mask; and

filtering the IP addresses using the subnet mask with a binary AND operator.

7.   A network comprising:

a visitor node having a browser program coupled to said network, said visitor node providing requests for information on said network;

a web site node having a respective web site responsive to requests for information from said visitor node to provide media content and data mining code to said visitor node;

a tracking node including a log file and a database, said tracking node responsive to a communication from said visitor node based upon said data mining code to store visitor data obtained from said visitor node into said log file; and

a filter node responsive to said visitor data based on a filter to select said visitor data for storage in a database,

whereby said database is accessible by an owner of said web site node to view relevant traffic data to the web site node.

8.   A network in accordance with claim 7, wherein said filter node selects said visitor data based on whether the visitor data is included within the filter.

9.   A network in accordance with claim 7, wherein said filter node selects said visitor data based on whether the visitor data is excluded from the filter.

10.   A network in accordance with claim 7, wherein said filter is an IP address filter.

11.   A network in accordance with claim 7, wherein said filter is a subnet mask applied to an IP address of the visitor node using an AND operator.

12.   A network in accordance with claim 7, wherein said filter uses classless inter-domain routing.

13.   A network in accordance with claim 7, wherein said filter uses standard pattern matching specifications like Regular Expressions.